



Agency Priority Goal | Action Plan | FY 23 – Q2

Strengthen Federal Cybersecurity

Goal Leader(s):

Matthew Hartman, Deputy Executive Assistant Director, Cybersecurity Division, Cybersecurity and Infrastructure Security Agency

Goal Overview

Goal statement

- Defend and secure the Federal Enterprise through a collaborative risk management effort with departments and agencies to coordinate risk response and interagency policy actions. By September 30, 2023, 50% percent of federal agencies will meet the end of year Binding Operational Directive-22-01 [Known Exploited Vulnerabilities] requirement for leveraging automated Continuous Diagnostics and Mitigation reporting and CISA will achieve measurable progress toward enhancing operational visibility within the Federal Civilian Executive Branches by improving asset discovery and vulnerability enumeration.

Problem to Be Solved

- Network visibility limitations due to encryption and cloud computing
- Constantly evolving threat landscape and rapid pace of change in the cyber domain compared to the pace of federal government policy generation and implementation
- The Federal Enterprise was not designed to be defended or managed as a single organization, and many federal agency networks are indefensible in part because they are decentralized. This decentralization creates obstacles for effective governance and for standardization of tools and services.
- Outdated and legacy technology poses risk of increased vulnerabilities associated with weak authentication exposure and unpatched software
- Technology investments are often not aligned with operational priorities for cyber defense

What Success Looks Like

- The Executive Order on Improving the Nation's Cybersecurity empowers DHS with additional authority to gain visibility into the federal enterprise and take action to safeguard systems
- Ramp up use of CISA-approved standardized tools and shared services to make federal networks more defensible and secure
- Agencies can identify threats and vulnerabilities and report on them using the Vulnerability Disclosure Program in advance of network disruptions
- CISA can identify cross-agency threats and vulnerabilities at the Federal Enterprise Level to provide a holistic view of the cyber threat, including access to host-level data and integration of data sources from across CISA's cyber programs

Goal target(s)

In the table below, please repeat the key metrics included in the goal statement (previous slide) that will be used to track progress.

Please update **this column** each quarter.

Achievement statement		Key indicator(s)	Quantify progress			Frequency
Repeat the achievement statement from the goal statement on the previous slide		A “key performance indicator” measures progress toward a goal target	These values enable us (and you!) to calculate % complete for <u>any</u> type of target*			When is there new data?
By...	We will...	Name of indicator	Target value	Starting value**	Current value	Update cycle
09/30/23	Achieve measurable progress toward enhancing operational visibility within the Federal Civilian Executive Branches by improving asset discovery and vulnerability enumeration.	Percent of federal agencies who meet Binding Operational Directive-22-01 [Known Exploited Vulnerabilities] automated reporting requirement for leveraging CDM reporting	50%		55%	Quarterly

* Even qualitative targets! If the target is to achieve a qualitative outcome, quantify progress this way: 1=“Yes, we achieved it”, 0=“No, not yet”

** As of 10/1/2021

Goal Strategies

Strategy 1: Lead Cyber Defense Operations

Respond to Threat Activity and Incidents

- Conduct and coordinate cyber defense operations to address the top active threats and mitigate critical vulnerabilities in the Federal Enterprise.
- Proactively detect, respond to, and mitigate risks of significant threat activity and critical vulnerabilities for these partners, and stop threats before disruption occurs and minimize the impact of incidents.

Mitigate Critical Vulnerabilities

- Mitigate critical vulnerabilities through reporting of software vulnerabilities, coordinating disclosure and patch development, and Federal Civilian Executive Branch (FCEB)-wide mitigation activities.



Strategy 2: Strengthen Cyber Risk Management

Proactive Risk Management

- Support Departments and Agencies to prioritize and manage strategic risks at an acceptable level, by working with partners to continuously prioritize their most significant risks and address them before network services are disrupted.
- Apply risk management, governance, and compliance principles at the Federal Enterprise level to see and manage strategic risks spanning across multiple agencies.

Take Responsibility for Risk

- As the Nation's risk advisor, ensure that the most significant risks to Mission Essential Functions are being addressed in a timely manner.



Strategy 3: Provide Cybersecurity Tools & Services

Provide Tools and Services

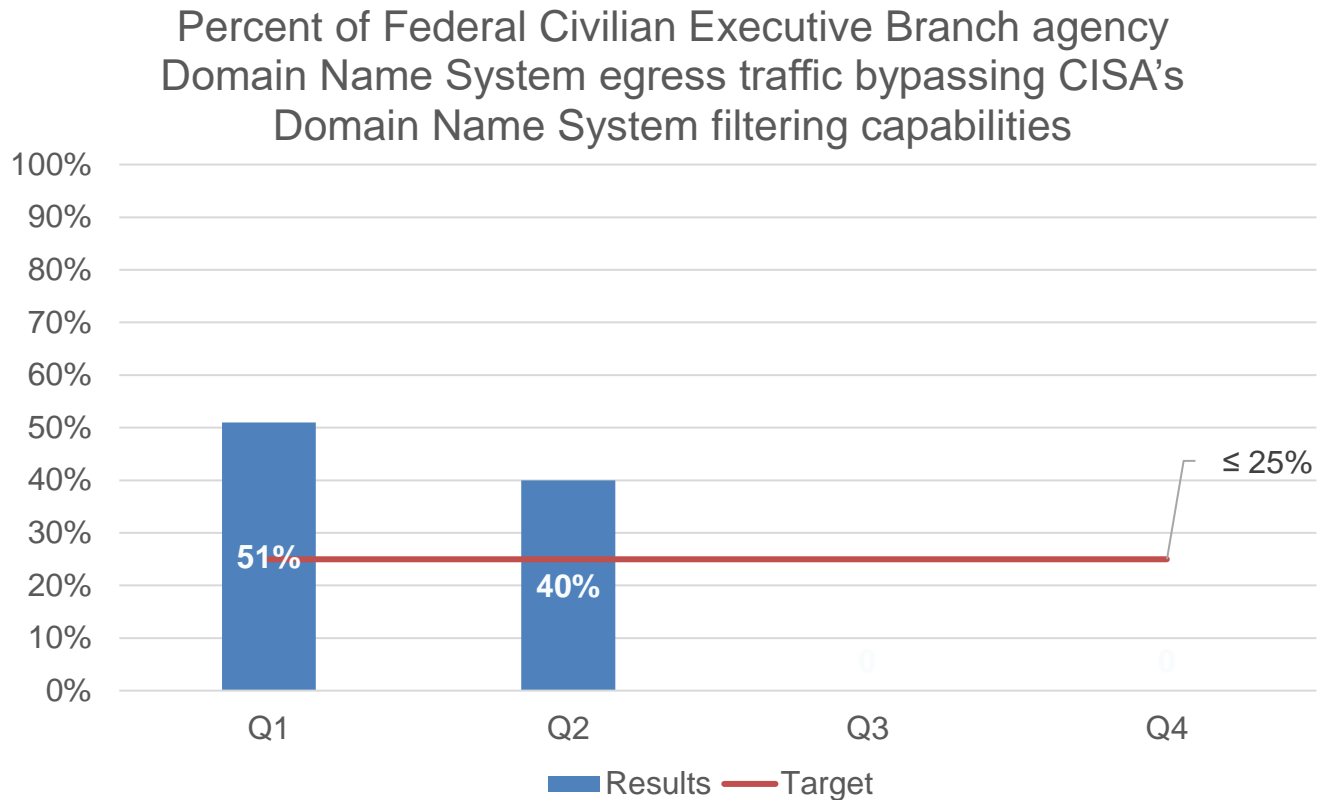
- Offer cybersecurity tools and services to FCEB agencies to assist them in achieving efficiencies, affordability, and standardization and quickly develop, deploy, and scale new services as needed. These tools and services address priority threats, provide situational awareness of risk postures, and build relationships in advance of an incident.
- Provide an adaptive suite of tools and services that demonstrably fill key gaps in managing priority strategic risks.

Manage Relationships/ Requirements

- Coordinate engagement with FCEB stakeholders to address priorities on cyber defense, risk management, and service needs and incorporate feedback into future service offerings.



Key indicators

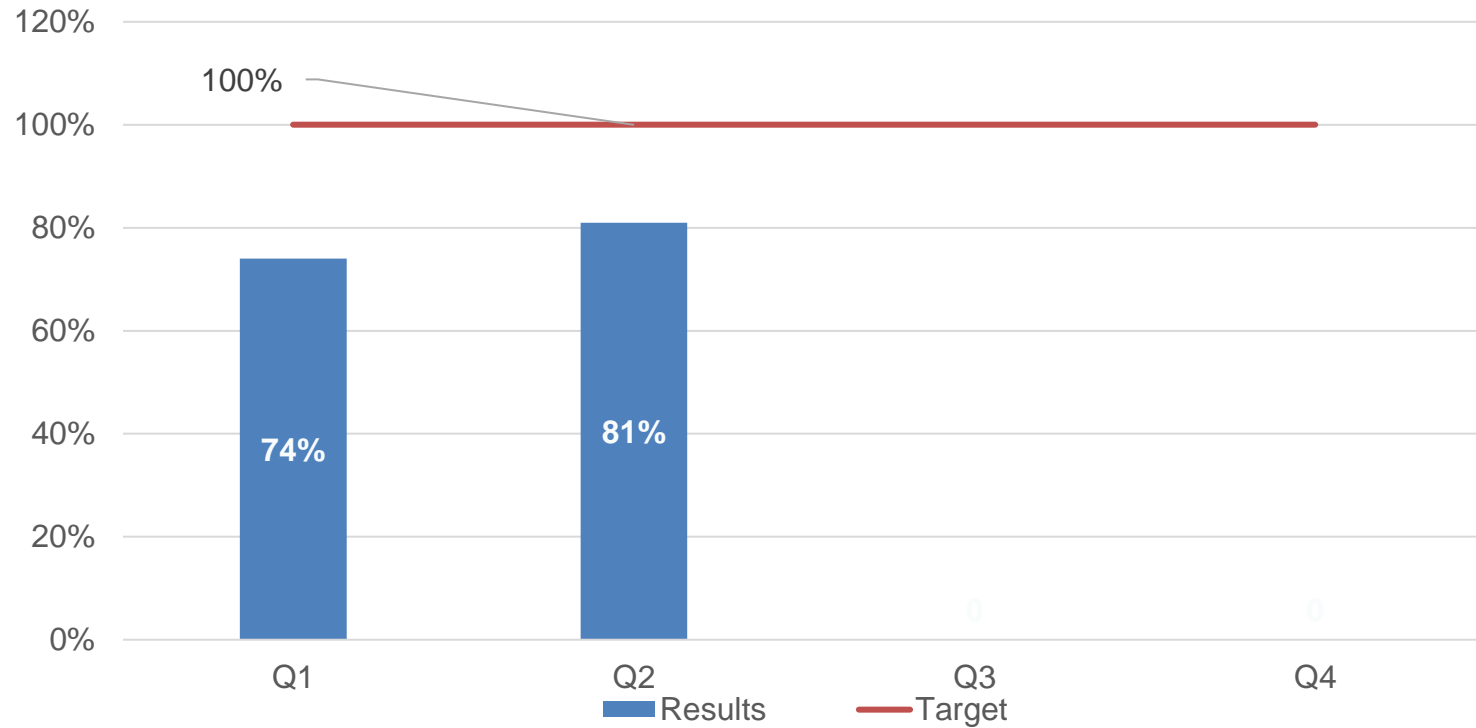


The percent of Federal Civilian Executive Branch (FCEB) Agency Domain Name System (DNS) egress traffic bypassing CISA's Domain Name System filtering capabilities continues to decrease. To better understand the stakeholder environment, CISA put out a data call requiring agencies to provide a status update on their bypass rules (including amount of traffic, number of endpoints, and if it includes high valued assets) to be submitted the first week of June for Q3. This will enable the team to gain a more complete picture of an agency's traffic. The issues from Q1 were resolved: one agency had missing data because they decommissioned their EINSTEIN collectors and two other agencies had missing data due to misconfigured circuits. Visibility has been restored.

Bypass Packets: 33573715271 / Total DNS Packets: 82939937366 = 40%

Key indicators

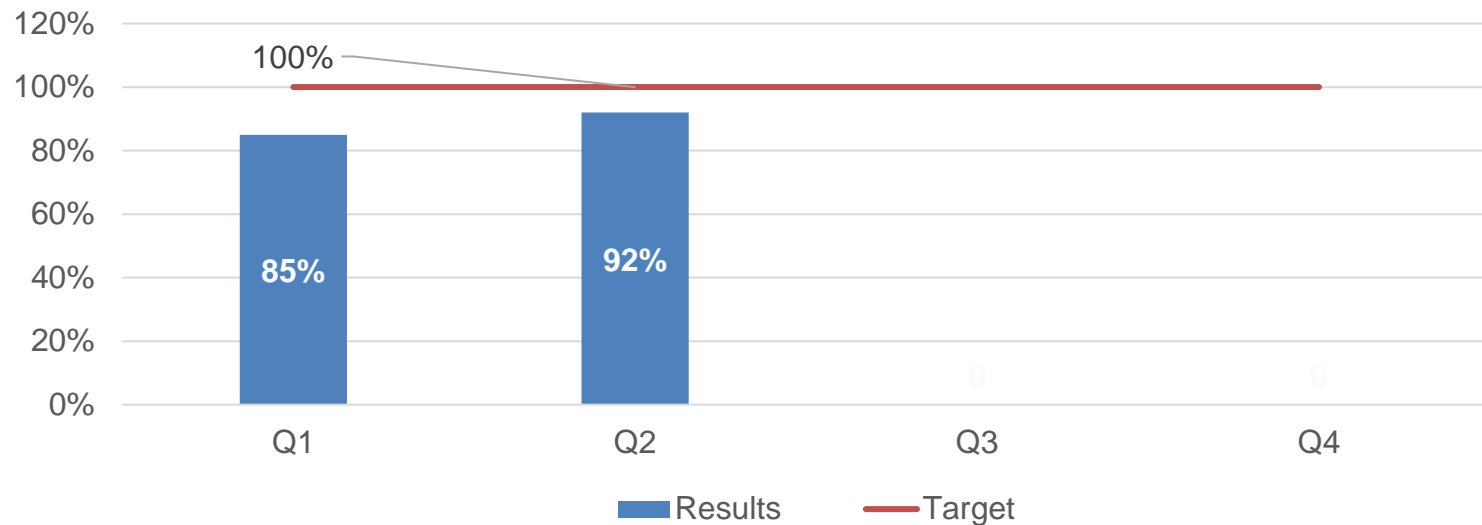
Percent of analytic capabilities transitioned to the Cloud Analytic Environment



By the end of Q2, 22 of 27 tools have completed migration to the Cloud Analytic Environment (81%). Five additional tools are in progress and are scheduled to be completed in Q3 and Q4.

Key indicators

Percent of agencies that have published a vulnerability disclosure policy that covers all agency internet accessible systems and services



All FCEB agencies have published a vulnerability disclosure policy (VDP) and 92% of agencies have a VDP with all systems in scope (93 out of 101 FCEB). CISA is making good progress toward their end of year target of 100% and continues efforts to bring all agencies into scope by performing regular domain scans and providing direct engagement to agencies who are not fully in scope.

Key indicators

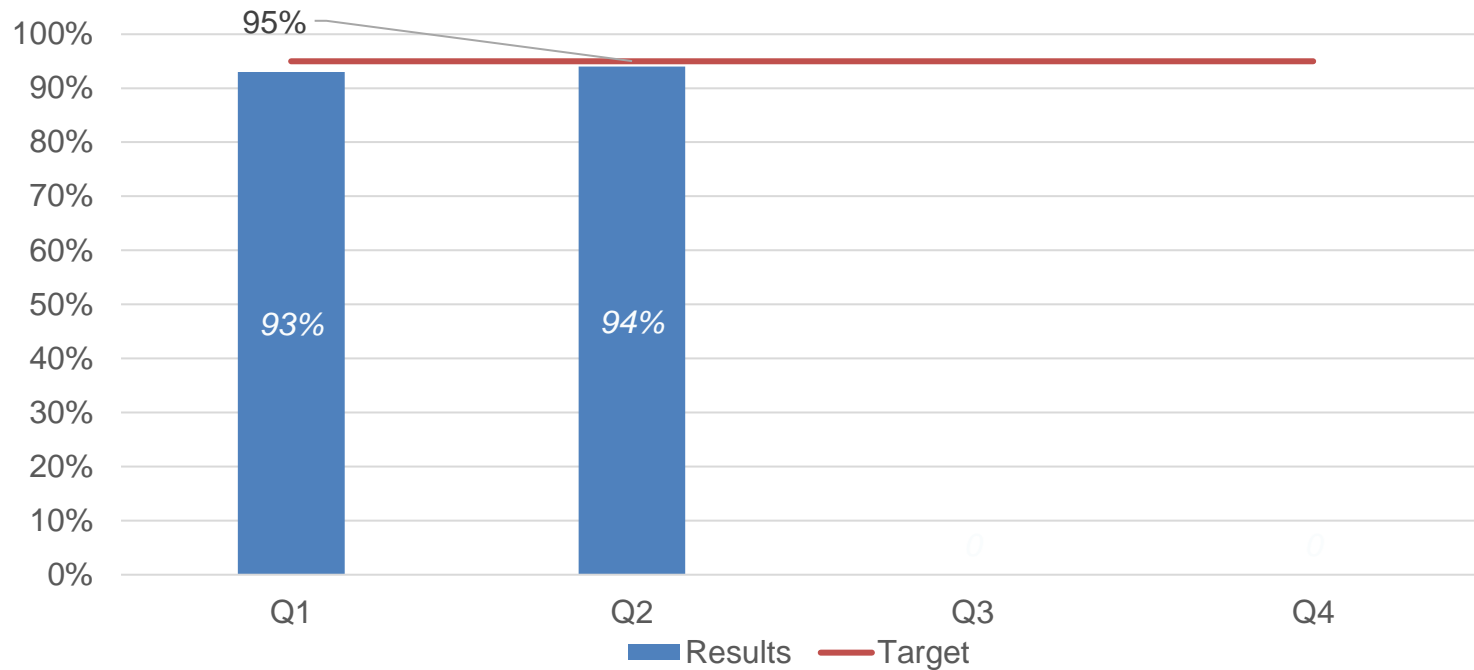
Percent of agencies that have initiated reporting of vulnerability enumeration performance data as required in Binding Operational Directive 23-01 [Asset Visibility] to the Continuous Diagnostics and Mitigation Federal Dashboard



Reporting to begin in Q3. Agencies have until April 3, 2023 - six months after the Binding Operational Directive (BOD 23-1) [Asset Visibility] was issued - to initiate the collection and reporting to the Continuous Diagnostics and Mitigation (CDM) Dashboard.

Key indicators

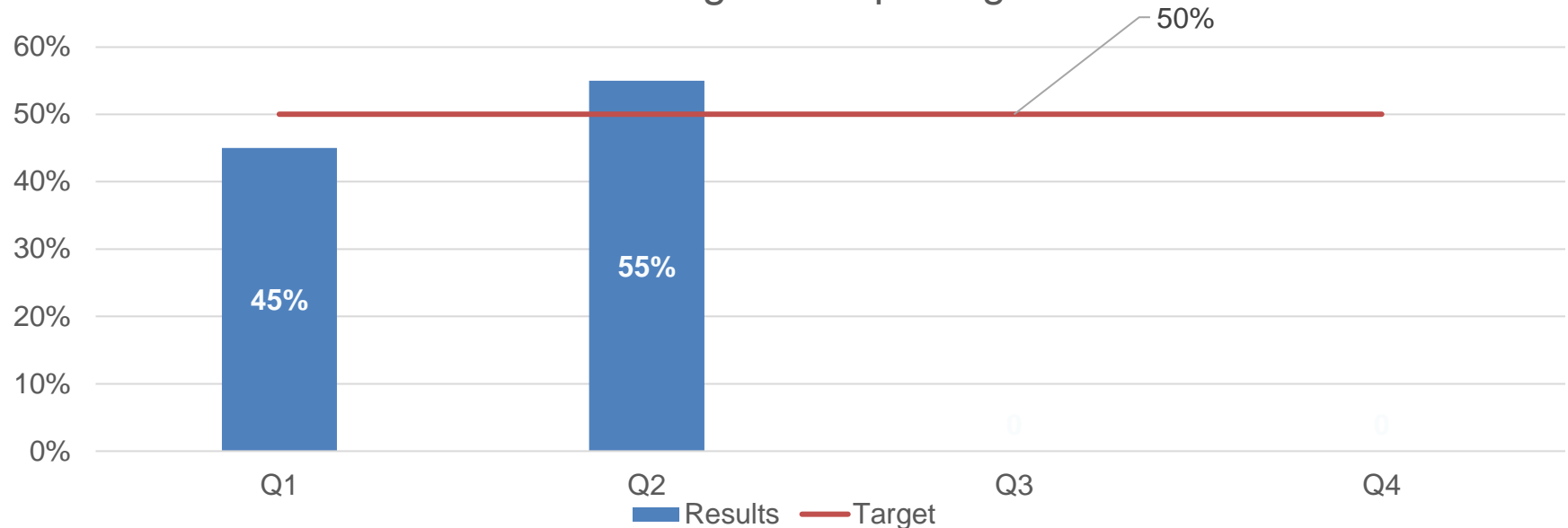
Percent of agencies that have developed internal vulnerability management and patching procedures by the specified timeline



As of FY23 Q2 reporting, 94% of federal agencies (95 of 101 FCEB) are in compliance, bringing CISA within striking distance of their annual target of 95%. While it is unlikely that CISA will ever achieve 100% for this particular measure, CISA continues to engage the remaining agencies. For example, in Q3, a training session will be conducted with the remaining 6%.

Key indicators

Percent of federal agencies who meet Binding Operational Directive-22-01 [Known Exploited Vulnerabilities] automated reporting requirement for leveraging Continuous Diagnostics and Mitigation reporting

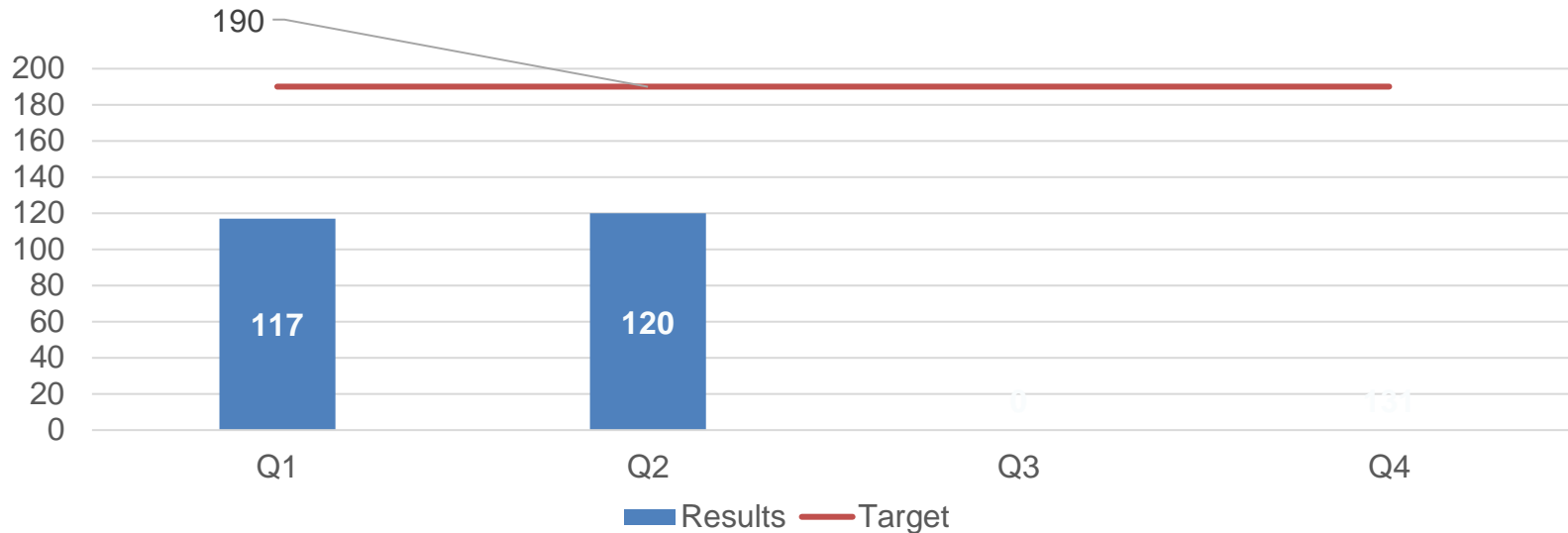


56 out of 101 FCEB meet the BOD-22-01 [Known Exploited Vulnerabilities (KEVs)] end-of-year coverage threshold.

CISA is performing well against this measure, with Q1 and Q2 results much higher than anticipated. However, we anticipate that factors like agency resourcing, prioritization and leadership changes will create challenges for achieving comprehensive CDM coverage as will CISA's inability to directly make changes to agency tooling. We foresee stabilized performance through the rest of FY23. Beyond FY23, CISA will be able to gain some incremental increases with agencies, likely as high as 85%, but may never approach 100%.

Key indicators

Number of voluntary adoptions of CISA Cybersecurity Shared Services offerings to federal civilian agencies



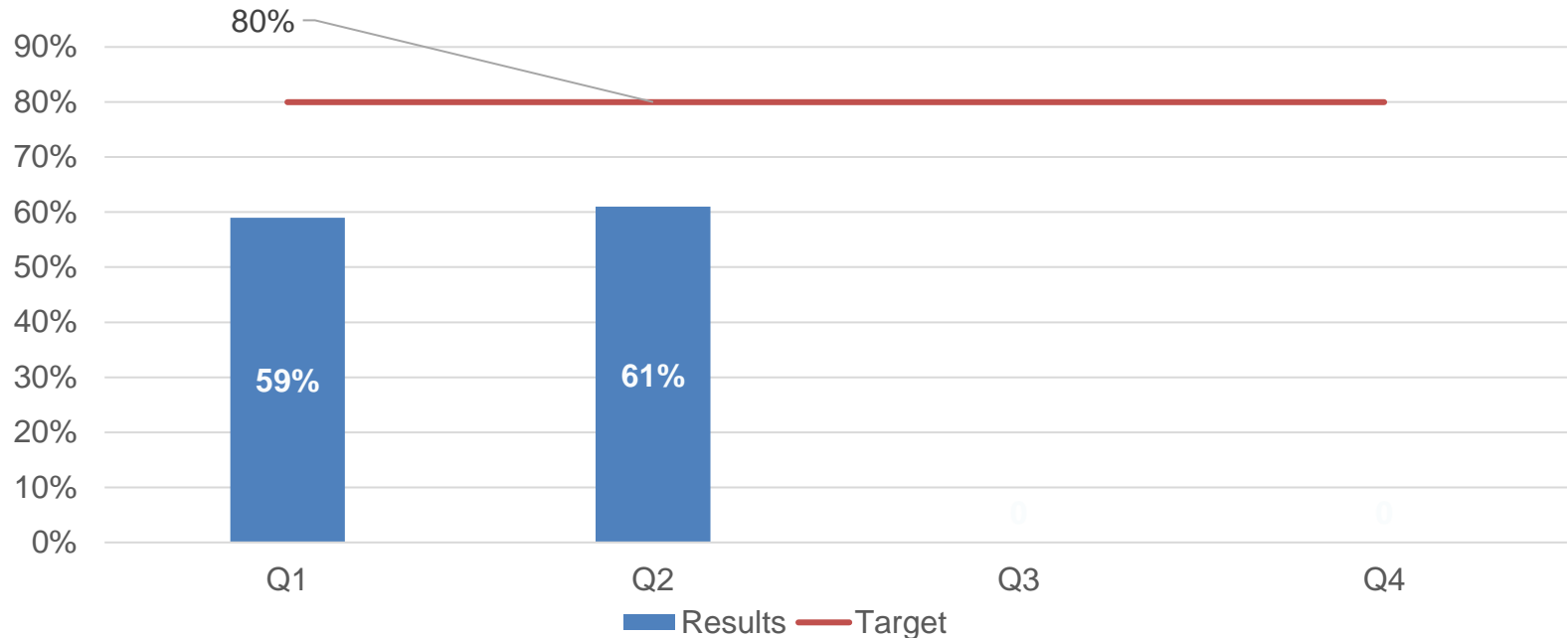
Number of Adoptions:

- Automated Indicator Sharing (AIS) 21
- Mobile Application Vetting (MAV) 10
- Shared Cybersecurity Services 54
- Traveler-Verified Information Protection 3
- Vulnerability Disclosure Policy Platform 32

This quarter saw the adoption of one Traveler-Verified Information Protection service and two for the Vulnerability Disclosure Policy Platform. CISA expects a big jump in voluntary adoptions over the coming two quarters and expects to meet the annual target of 190 adoptions. Key activities that we anticipate will positively impact this measure include the incorporation of the SCuBA service, the completion of the rebrand of AIS, and an expected increase in MAV licenses.

Key indicators

Percent of endpoints from federal agencies covered by Endpoint Detection and Response solutions that are deployed by Continuous Diagnostics and Mitigation



Q2 results are based on 554,660 Endpoint Detection and Response (EDR) tools/agents deployed of 909,716 EDR Requests For Service (RFS) received, covering all agencies with CDM EDR deployments (~40 as of the start FY23).

Key milestones

Milestone Summary				
#	Key Milestone	Milestone Due Date	Milestone Status	Comments
1.1	Conduct program increment planning session to plan the migration of the remaining on-premises analytic capabilities to the Cloud Analytic Environment	Q2	Complete	Mission Engineering conducted Program Increment Planning for Quarter 2 (PI 23.2) January 23- January 27, 2023. The PI 23.2 Release Planning Review was successfully conducted on Wednesday, 1 February 2023. The next program increment planning session is scheduled for April 24 - April 28, 2023 for Quarter 3.
2.1	100% of agencies with a CDM Memorandum of Agreement (MOA) have deployed the CDM Dashboard and are feeding data to CISA	Q2	Complete	93/93 MOA agencies have deployed the CDM Dashboard and are feeding data to CISA. These include the 64 (of 74 total) DEFEND-F agencies that have MOAs with CDM. CDM plans to continue its efforts (currently approximately 18 months long) to make contact with the remaining ten DEFEND-F agencies.
2.2	Reach 93% of federal agencies that have developed internal vulnerability management and patching procedures in compliance with CISA-provided scope and timelines	Q3	Complete	Agencies made more progress in Q1 than anticipated, allowing this milestone to be complete ahead of schedule.

Key milestones

Milestone Summary				
#	Key Milestone	Milestone Due Date	Milestone Status	Comments
2.3	Develop a draft Asset Visibility Capacity Enhancement Guide to signal best practices and assist agencies with implementation of the expected Asset Visibility directive requirements	Q1	Complete	A draft Asset Visibility Enhancement Guide has been completed to signal best practices and assist agencies with implementation of the expected Asset Visibility directive requirements.
3.1	Complete the first wave of EDR deployments (4 CFO Act; 12 non-CFO Act agencies) and initiate the second wave (5 CFO Act; ~25 non-CFO Act agencies)	Q2	Complete	This milestone was completed on schedule. As of Q2, CISA has completed the first wave of deployments with four CFO Act Agencies (SBA, SSA, HUD, and DHS) and 23 non-CFO Act agencies. There are nine CFO Act Agencies currently in deployment with CISA. They include (DOC, DOE, DOJ, DOL, Education, HHS, NASA, Treasury, and USAID). CISA is also in the process of deploying to six additional non-CFO Act agencies.

Narrative

Overall, CISA has made progress towards its FY23 targets, and all milestones are complete, with one that was completed ahead of schedule.

Notable accomplishments include:

- *Percent of federal agencies who meet BOD-22-01 [Known Exploited Vulnerabilities (KEVS)] automated reporting requirement for leveraging CDM reporting* – met its target in Q2, ahead of schedule, with results much higher than anticipated.
- *Percent of Federal Civilian Executive Branch Agency Domain Name System egress traffic bypassing CISA's Domain Name System filtering capabilities* has continued to decrease in FY23 Q1, from 51% to 40% for FY23 Q2 due to the increase in adoption of protective DNS by FCEB agencies.
- *Number of voluntary adoptions of CISA cybersecurity shared services offerings to federal civilian agencies.* CISA expects a big jump in voluntary adoptions over the next two quarters and expects to meet the annual target of 190 adoptions. Key activities that we anticipate will positively impact this measure include the incorporation of the SCuBA service, the completion of the rebrand of AIS, and an expected increase in MAV licenses.